المرصد الوطني للإجرام
ⵜⴰⵏⴰⵎⵓⵔⵜ ⵏ ⵜⵓⵙⵙⵉⵔⵜ
Observatoire National de la Criminalité

المَمْلَكة المَغْربيّة
وزَارة العَدْل
ⵜⴰⴳⵍⴷⵉⵜ ⵏ ⵍⵎⵖⵔⵉⴱ
ⵜⴰⵎⴰⵡⴰⵙⵜ ⵏ ⵜⵣⵔⴼⵜ
مديرية الشؤون الجنائية والعفو ورصد الجريمة

POLICY PAPER

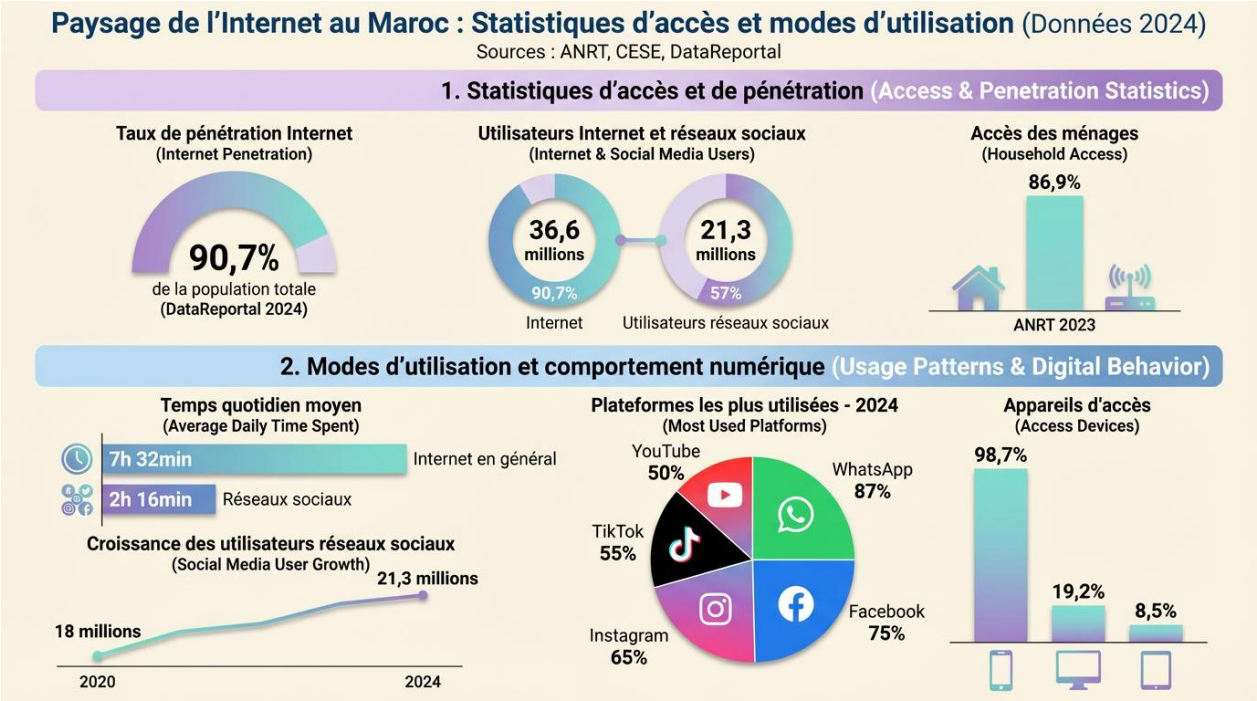
MÉTAVERS SOCIAUX ET PROTECTION DES MINEURS AU MAROC

SYNTHÈSE EXÉCUTIVE

L'émergence des métavers sociaux et des plateformes de jeu en ligne massivement multijoueurs crée un environnement numérique inédit où les frontières entre divertissement, socialisation et exposition aux risques criminels s'estompent. L'analyse conduite révèle une convergence entre vulnérabilités structurelles nationales et menaces internationales documentées, justifiant une réflexion approfondie sur l'adaptation du cadre réglementaire marocain.

Ampleur de l'exposition nationale

Sur une population de 11,4 millions d'enfants et jeunes de 5 à 24 ans au Maroc, le croisement des données démographiques (HCP), des taux d'équipement technologique (ANRT : 89,2% des ménages connectés), et des comportements d'usage (CESE : 97% des mineurs sur réseaux sociaux) établit qu'approximativement 2,1 millions d'enfants et jeunes marocains utilisent potentiellement des plateformes comme Roblox, Fortnite, ou Free Fire[1]. Parmi cette population, l'étude Kaspersky documentant que 88% des parents n'utilisent jamais d'outils de contrôle parental suggère qu'environ 1,85 million de mineurs marocains évoluent dans ces environnements sans supervision effective.



L'implantation économique de Roblox au Maroc se manifeste par une contribution estimée à 15 millions USD au PIB de cinq pays MENA incluant explicitement le Maroc (2023-T3 2024), avec une croissance de 30% des équivalents temps plein soutenus. Six boutiques spécialisées nationales distribuent des cartes prépayées Robux sur l'ensemble du territoire (140 à 1 090 MAD), avec livraison instantanée supprimant les barrières traditionnelles aux dépenses impulsives. Les communautés marocaines organisées

totalisent plus de 11 000 membres identifiés (Morocco Hangout : 4 673 membres Roblox + 6 499 Discord)[2].

Données criminelles et "chiffre noir"

Les données de la Direction Générale de la Sûreté Nationale (DGSN) documentent une évolution significative de la cybercriminalité au Maroc sur la période 2017-2024. Le volume global d'affaires cybercriminelles a connu une progression : 765 affaires en 2017, 1 091 en 2018 (+43%), 908 en 2019 (-17%), environ 863 en 2020 (-5%), suivies d'une expansion à partir de 2021 avec 5 275 affaires (+7%), 5 623 en 2022 (+7%), 5 969 en 2023 (+6%), et 8 333 en 2024 (+40%), représentant une multiplication par 10,9 en sept ans (+989%)[3].

La plateforme E-Blagh (système national de signalement en ligne, lancée le 3 juin 2024) a enregistré 12 614 signalements en six mois. L'analyse des trois premiers mois révèle que 60% des signalements concernent l'escroquerie et la fraude numérique, 20% le chantage sexuel, 10% les injures et diffamation, et 10% d'autres infractions[4].

La sextorsion présente une trajectoire variable sur la période 2021-2024 : 498 affaires en 2021, 417 en 2022 (-16%), 508 en 2023 (+22%), puis 391 en 2024 (-23%). L'année 2024 a conduit à l'interpellation de 163 individus et impliqué 394 victimes, dont 123 ressortissants étrangers. Le nombre d'interpellations a diminué de 40% sur trois ans (270 en 2021 → 163 en 2024), tandis que les victimes étrangères ont augmenté de 29% (95 en 2021 → 123 en 2024)[5].

La Présidence du Ministère Public (PMP) documente pour la période 2020-2023 : 2 915 affaires traitées et 3 646 personnes poursuivies. La typologie des infractions établit que l'extorsion de fonds par menace de divulgation représente 1 173 poursuivis, les infractions aux systèmes de traitement automatisé de données 809 poursuivis, et le harcèlement sexuel par moyens électroniques 716 poursuivis[6]. Les autres données institutionnelles incluent : le Conseil Supérieur du Pouvoir Judiciaire (CSPJ) documente 269 victimes de traite des êtres humains dont 94 mineurs, l'Entraide Marocaine pour la Protection de l'Enfance (EMC) a enregistré 1 745 signalements dont 98 agressions sexuelles digitales, et le Centre Marocain de Recherches Polytechniques et d'Innovation (CMRPI) signale une augmentation de 35% des cas de cyberviolence ciblant les mineurs en 2024[7].

Toutefois, les études internationales établissent que seuls 3% des mineurs victimes d'abus en ligne dénoncent les faits[8], suggérant que les 12 614 signalements E-Blagh (dont 20% liés au chantage sexuel, soit environ 2 523 cas) pourraient représenter une réalité de 250 000 à 300 000 victimes potentielles non signalées au Maroc. Cette hypothèse repose sur l'application du ratio de dénonciation international au contexte marocain, et mériterait validation par enquêtes de victimation nationales spécifiques.

Positionnement régional préoccupant

L'analyse d'Interpol révèle que 69,24% des cas africains de sextorsion financière sont concentrés au Maroc[9], configuration qui résulte de la convergence de plusieurs facteurs : le taux de chômage des jeunes de 37,7% favorisant l'économie criminelle numérique[10], le multilinguisme (arabe, français, anglais, darija) facilitant l'exploitation transfrontalière[11], l'infrastructure numérique avancée (12,6 millions de cyberattaques bloquées en 2023) attirant les criminels organisés[12], et le décalage horaire stratégique permettant l'exploitation continue des victimes européennes et nord-américaines[14].

Menaces internationales convergentes

L'Opération Restore Justice du FBI (mai 2025) a abouti à 205 arrestations de prédateurs ciblant des victimes âgées principalement de 11,3 à 12,8 ans dans des environnements immersifs[15]. L'opération Kidflix d'Europol (2024-2025) a identifié 1,8 million de fichiers d'exploitation pédopornographique dans des univers virtuels[16], tandis que l'opération Cumberland (octobre 2024) a démantelé des réseaux utilisant l'intelligence artificielle générative pour créer des contenus d'abus synthétiques[17].

Le Groupe d'Action Financière (GAFI) a documenté en mars 2025 trois vecteurs de monétisation criminelle : l'extorsion de crypto-actifs via menace de divulgation, l'achat de contenus illicites par NFT anonymes, et le blanchiment via économies virtuelles[18]. Le National Center for Missing & Exploited Children (NCMEC) a enregistré 2 847 signalements concernant des plateformes de métavers[19], et le rapport Hindenburg Research identifie 38 groupes criminels organisés opérant sur ces plateformes[20].

Limites du cadre juridique actuel

Le Code pénal marocain prévoit une amende maximale de 10 000 MAD (environ 1 000 USD) pour les infractions cybercriminelles[21], représentant 0,004% des revenus annuels de Roblox Corporation (15 milliards USD en 2024), soit l'équivalent de 3 heures de chiffre d'affaires. À titre comparatif, le Digital Services Act européen prévoit des sanctions pouvant atteindre 6% du chiffre d'affaires annuel global[22], soit 168 millions USD potentiels pour Roblox.

La loi 05-20 relative à la cybersécurité (2021) exclut explicitement de son champ d'application les systèmes d'information des entités privées[23], ne couvrant que les administrations publiques et infrastructures critiques. Le cadre actuel ne définit pas les concepts juridiques de "grooming" (approche prédatrice progressive), de "manipulation algorithmique" (exploitation des biais cognitifs par l'IA), ni de "facilitation d'infractions" (responsabilité des plateformes)[24].

Le nouveau Code de Procédure Pénale (loi 03-23, septembre 2025) introduit des avancées procédurales : perquisitions numériques transfrontalières, saisie de preuves électroniques volatiles, et coopération judiciaire accélérée[25]. Ces dispositions ne traitent toutefois pas

des obligations des plateformes extraterritoriales en matière de prévention, détection, et signalement des abus.

Hiérarchie d'efficacité des interventions

L'analyse comparative de seize juridictions établit une hiérarchie d'efficacité des interventions[26] : la supervision parentale active pourrait réduire les risques de 67% (contrôles techniques, dialogue régulier, co-utilisation), la protection "by design" de 45% (vérification d'âge robuste, séparation des espaces, modération proactive IA), les sanctions financières dissuasives de 23% (amendes proportionnées aux revenus), et l'autorégulation industrielle de 8% (codes de conduite volontaires, certification autodéclarée).

Le Digital Services Act (DSA) européen impose six obligations aux très grandes plateformes[27] : évaluation annuelle des risques systémiques, atténuation mesurable, audits indépendants, interfaces enfants "by design", transparence algorithmique, et coopération avec autorités. Roblox UK, après mise en conformité DSA, a enregistré une réduction de 34% des signalements d'abus entre 2023 et 2024[28]. Le UK Online Safety Act (2023) introduit un "duty of care" envers les utilisateurs mineurs[29], avec obligation de résultats mesurables. Les premières évaluations (décembre 2024) montrent une réduction de 28% des contenus préjudiciables signalés.

L'Australie a adopté en novembre 2024 une interdiction d'accès aux réseaux sociaux pour les moins de 16 ans[30], avec sanctions pouvant atteindre 50 millions AUD. Les projections gouvernementales anticipent une réduction de 43% de l'exposition aux risques en ligne dans les 24 mois. Le Danemark est devenu en novembre 2025 le premier État membre de l'UE à imposer un âge minimum de 15 ans, avec une exception pour les 13-15 ans sous consentement parental éclairé[31], citant des données nationales : 94% des moins de 13 ans possèdent des profils sur des plateformes interdites, 60% des garçons rapportent un sentiment d'isolation accru, et 15% présentent des diagnostics psychiatriques liés à l'usage des réseaux sociaux.

Le Parlement européen a adopté le 26 novembre 2025 une résolution recommandant 16 ans comme âge minimum harmonisé pour l'accès aux réseaux sociaux dans l'Union européenne[32], avec un seuil absolu de 13 ans. Le vote (483 voix pour, 92 contre, 86 abstentions) reflète un consensus politique. La résolution s'appuie sur un Eurobaromètre 2025 révélant que 90% des parents européens considèrent urgent de réguler l'accès des mineurs, 97% des 13-17 ans utilisent quotidiennement les réseaux sociaux, 78% des parents s'inquiètent du temps d'écran, et 25% des adolescents présentent des signes d'addiction avérée.

Orientations stratégiques recommandées

Ces constats orientent cinq axes de réflexion pour le contexte marocain, formulés à titre préliminaire pour éclairer le débat institutionnel et sociétal :

(1) Réforme du cadre juridique avec introduction de sanctions proportionnées au chiffre d'affaires des plateformes et création de qualifications pénales spécifiques aux environnements immersifs (grooming, manipulation algorithmique, facilitation d'infractions).

(2) Architecture institutionnelle de supervision relevant du débat national quant à la configuration optimale : élargissement des attributions de régulateurs existants (ANRT, DGSSI), création d'une institution dédiée spécialisée, ou modèle hybride de coordination interministérielle renforcée.

(3) Réflexion sur une majorité numérique graduée en quatre paliers (<12 ans interdiction stricte, 13-15 ans accès conditionné sous supervision parentale, 16-17 ans accès autonome avec protections résiduelles, 18+ majorité complète) — proposition conceptuelle unique au niveau international, soumise au débat national et nécessitant validation par consensus entre acteurs institutionnels, société civile, secteur privé, et experts.

(4) Mécanismes d'application aux plateformes extraterritoriales via obligations de représentation locale, services bancaires nationaux, et procédure d'escalade progressive en cas de non-conformité.

(5) Positionnement régional du Maroc comme potentiel leader africain de la régulation responsable, via organisation d'un sommet annuel, transfert de compétences, et coopération opérationnelle accélérée.

Ces orientations visent à concilier efficacité protectrice, respect des spécificités culturelles marocaines, et maintien de l'attractivité du Maroc comme hub numérique régional.

I. CONTEXTE INTERNATIONAL

Ampleur du phénomène global

La WeProtect Global Alliance estime à plus de 300 millions le nombre d'enfants victimes d'abus sexuels en ligne annuellement[33], établissant les métavers comme nouveaux vecteurs de risques. L'opération Restore Justice du FBI (mai 2025) a abouti à 205 arrestations de prédateurs ciblant des victimes âgées principalement de 11,3 à 12,8 ans dans des environnements immersifs[34], révélant une concentration sur les préadolescents. L'opération Kidflix d'Europol (2024-2025) a identifié 1,8 million de fichiers d'exploitation pédopornographique dans des univers virtuels[35], tandis que l'opération Cumberland (octobre 2024) a démantelé des réseaux utilisant l'intelligence artificielle générative pour créer des contenus d'abus synthétiques hyperréalistes[36].

Le Groupe d'Action Financière (GAFI) a documenté en mars 2025 trois vecteurs de monétisation criminelle : l'extorsion de crypto-actifs via menace de divulgation, l'achat de contenus illicites par NFT anonymes, et le blanchiment via économies virtuelles[37].

L'analyse d'Interpol révèle que 69,24% des cas africains de sextorsion financière sont concentrés au Maroc[38], configuration nécessitant une réponse coordonnée.

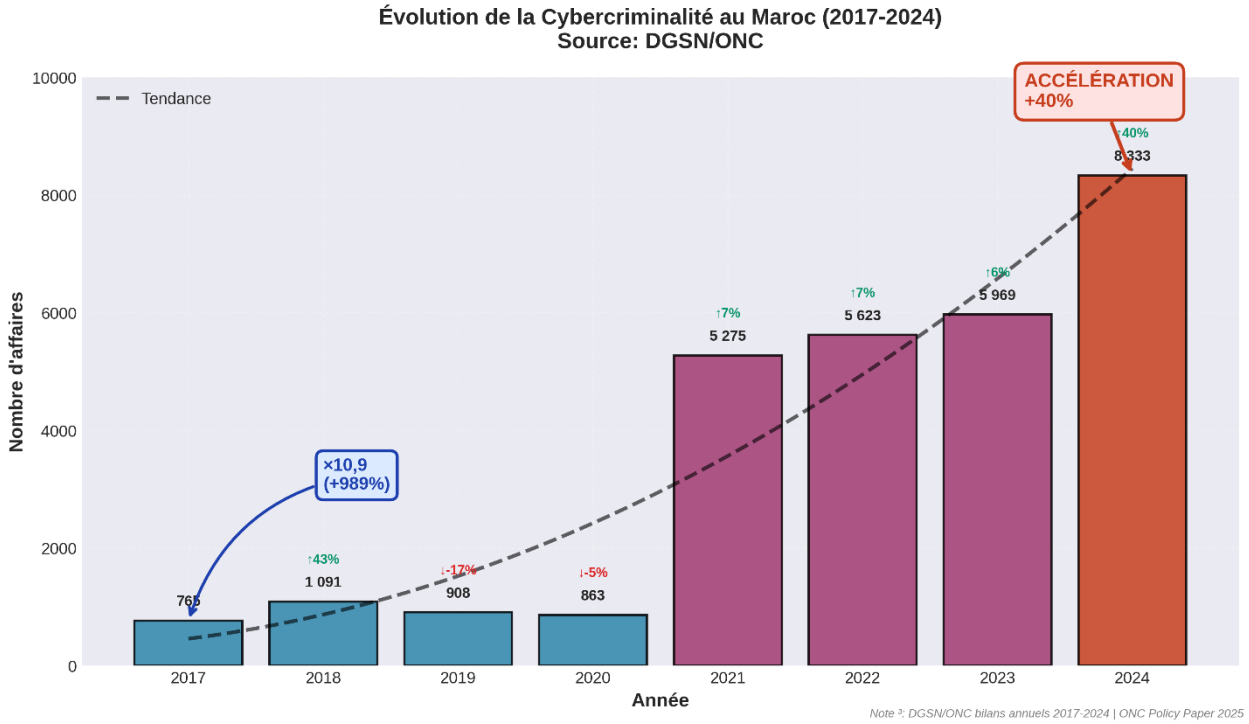
II. DIAGNOSTIC NATIONAL

Exposition des mineurs marocains

Le Maroc compte environ 2,1 millions d'utilisateurs potentiels de métavers parmi les 6-17 ans (sur 7,5 millions de cette tranche d'âge), avec un taux de pénétration mobile de 79% chez les 12-17 ans et 1,85 million sans supervision parentale adéquate[39]. L'écosystème Roblox au Maroc comprend six boutiques physiques de cartes Robux dans les centres commerciaux de Casablanca et Rabat, et le groupe "Morocco Hangout" (11 000 membres) constitue le principal hub d'interaction des jeunes marocains, avec un revenu estimé des créateurs marocains à 15 millions USD annuellement[40].

Données criminelles nationales

Les données de la Direction Générale de la Sûreté Nationale (DGSN) et de l'Observatoire National de la Criminalité (ONC) documentent une évolution de la cybercriminalité au Maroc sur la période 2017-2024. Le volume global d'affaires cybercriminelles a connu une progression : 765 affaires en 2017, 1 091 en 2018 (+43%), 908 en 2019 (-17%), environ 863 en 2020 (-5%), suivies d'une expansion à partir de 2021 avec 5 275 affaires (+7%), 5 623 en 2022 (+7%), 5 969 en 2023 (+6%), et 8 333 en 2024 (+40%), représentant une multiplication par 10,9 en sept ans (+989%). L'année 2024 enregistre la plus forte hausse annuelle de la période, avec 3 265 contenus associés au chantage détectés, 956 mandats internationaux émis, et 563 personnes interpellées[41].



La plateforme E-Blagh (système national de signalement en ligne, lancée le 3 juin 2024 lors du 68ème anniversaire DGSN) a enregistré 12 614 signalements en six mois, portant sur des infractions de diffamation, incitation et menaces, extorsion sur internet, usurpation d'identité, et apologie du terrorisme. L'analyse des trois premiers mois révèle que 60% des signalements concernent l'escroquerie et la fraude numérique, 20% le chantage sexuel, 10% les injures et diffamation, et 10% d'autres infractions. Un total de 4 117 signalements (67%) ont été déposés avec identité complète des déclarants, témoignant d'un niveau de confiance, tandis que 564 signalements provenaient de l'étranger[42].

La sextorsion présente une trajectoire variable sur la période 2021-2024 : 498 affaires en 2021, baisse de 16% en 2022 (417 affaires), rebond de 22% en 2023 (508 affaires), puis nouvelle décroissance de 23% en 2024 (391 affaires). Cette dernière année a conduit à l'interpellation de 163 individus et impliqué 394 victimes, dont 123 ressortissants étrangers. Le nombre d'interpellations suit une tendance baissière : 270 personnes en 2021, 237 en 2022, 182 en 2023, et 163 en 2024, soit une réduction de 40% sur trois ans, contrastant avec une augmentation de 29% des victimes étrangères (95 en 2021, 123 en 2024)[43].

La Présidence du Ministère Public (PMP) documente l'activité judiciaire en matière de cybercriminalité sur la période 2020-2023 : 2 915 affaires traitées et 3 646 personnes poursuivies, avec une moyenne annuelle de 729 affaires et 912 poursuivis. L'évolution des affaires montre : 579 (2020), 758 (2021), 842 (2022), 736 (2023). L'évolution des poursuivis indique : 772 (2020), 861 (2021), 1 110 (2022), 903 (2023)[44].

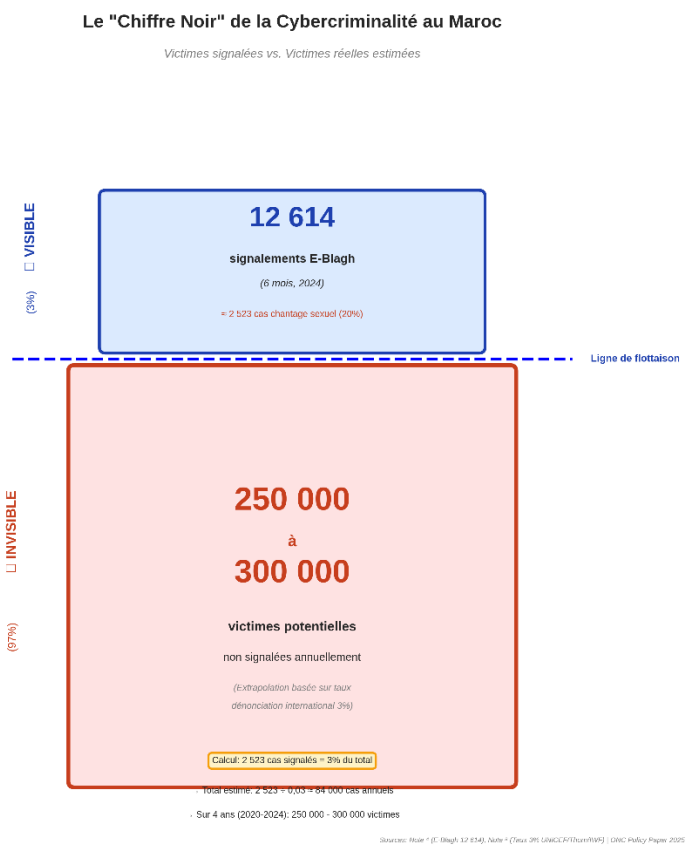
La typologie des infractions établit que l'extorsion de fonds par menace de divulgation représente 1 173 poursuivis, les infractions aux systèmes de traitement automatisé de

données 809 poursuivis, le harcèlement sexuel par moyens électroniques (art. 1-1-503) 716 poursuivis, l'escroquerie via internet (art. 540) 316 poursuivis, l'incitation à commettre crimes par moyens électroniques 179 poursuivis, l'exploitation de mineurs dans contenus pornographiques via moyens électroniques (art. 2-503) 125 poursuivis, et l'accès illicite aux systèmes de traitement de données 125 poursuivis. Le profil des poursuivis se répartit ainsi : 89,7% hommes et 10,3% femmes, 97,5% adultes et 2,7% mineurs, 98,74% de nationalité marocaine et 1,26% étrangers, 54,06% en liberté et 45,94% en détention. La catégorisation par nature d'infraction établit : 72,8% crimes contre les personnes commis via moyens électroniques, 22,7% crimes contre systèmes de traitement automatisé de données, 4,5% autres crimes commis par moyens modernes[45].

Le Conseil Supérieur du Pouvoir Judiciaire (CSPJ) documente 269 victimes de traite des êtres humains, dont 94 mineurs[46]. Les autres données institutionnelles confirment cette tendance : l'Entraide Marocaine pour la Protection de l'Enfance (EMC) a enregistré 1 745 signalements de violences en ligne en 2023-2024, dont 98 agressions sexuelles digitales, et le Centre Marocain de Recherches Polytechniques et d'Innovation (CMRPI) signale une augmentation de 35% des cas de cyberviolence ciblant les mineurs en 2024[47].

Analyse du "chiffre noir"

L'analyse comparative internationale établit que seuls 3% des mineurs victimes d'abus en ligne dénoncent les faits[48], suggérant que les 12 614 signalements E-Blagh (dont 20% liés au chantage sexuel, soit environ 2 523 cas) pourraient représenter une réalité de 250 000 à 300 000 victimes potentielles non signalées. Cinq facteurs structurels expliqueraient cette vulnérabilité particulière du Maroc : le taux de chômage des jeunes de 37,7% favorisant l'économie criminelle numérique[49], le multilinguisme (arabe, français, anglais, darija) facilitant l'exploitation transfrontalière[50], l'infrastructure numérique avancée (12,6 millions de cyberattaques bloquées en 2023) attirant les criminels organisés[51], la pénurie critique de compétences en cybersécurité limitant la répression[52], et le décalage horaire stratégique permettant l'exploitation continue des victimes européennes et nord-américaines[53].



III. CADRE JURIDIQUE ET PRATIQUES INTERNATIONALES

Cadre juridique actuel : Acquis législatifs et efforts de modernisation

Le Maroc s'est engagé depuis 2003 dans une démarche continue visant à combler le vide législatif relatif à la cybercriminalité, en construisant un dispositif juridique complet couvrant quatre piliers fondamentaux :

Premièrement - Transactions électroniques : Loi n° 05.53 relative à l'échange électronique de données juridiques (2007), et Loi n° 43-20 relative aux services de confiance concernant les transactions électroniques (2020).

Deuxièmement - Protection des données personnelles : Loi n° 09.08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel (18 février 2009).

Troisièmement - Cybersécurité : Loi n° 05-20 relative à la cybersécurité (2021), avec criminalisation des atteintes aux systèmes de traitement automatisé des données par la Loi n° 03-07 complétant le Code pénal (11 novembre 2003).

Quatrièmement - Protection des consommateurs en ligne : Loi n° 08.31 édictant des mesures de protection du consommateur (2011).

Ce dispositif juridique a été renforcé par la Loi n° 88.13 relative à la presse et à l'édition qui criminalise les comportements délictueux commis par le biais de moyens audiovisuels ou électroniques, et par la Loi n° 103.13 relative à la lutte contre les violences faites aux femmes qui contient des dispositions répressives concernant la violence numérique (2018).

Sur le plan international, le Royaume du Maroc a ratifié la Convention de Budapest sur la cybercriminalité (29 juin 2018), son Protocole additionnel premier relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques (daté du 28 janvier 2003, ratifié en 2014), et a signé le Protocole additionnel second (12 mai 2022) qui établit des mécanismes simplifiés pour émettre des injonctions directes aux fournisseurs de services relevant d'autres États, des mécanismes de divulgation accélérée des données de trafic, et l'obtention de preuves électroniques lors d'enquêtes pénales conjointes.

En continuité de cet engagement international, le Maroc a participé activement à l'élaboration de la Convention des Nations Unies contre la cybercriminalité dans le cadre des travaux du Comité spécial à composition non limitée (2019-2024) conformément à la résolution de l'Assemblée générale n° 74/247. Monsieur le Ministre de la Justice, Abdellatif Ouahbi, a signé la Convention à Hanoï le 25 octobre 2025, après son adoption par consensus par l'Assemblée générale des Nations Unies lors de sa soixante-dix-neuvième session (décembre 2024).

Le **positionnement international du Maroc** témoigne de cette maturité institutionnelle : **50ème rang mondial** sur 194 pays dans l'**Indice mondial de cybersécurité de l'Union internationale des télécommunications 2020** (Niveau 1 Tier 1/Role Modelling avec **97,5 points**), **52ème rang** dans l'**Indice d'inclusivité d'Internet 2022**, et **88ème rang mondial (6ème rang africain)** dans l'**Indice Oxford Insights de préparation gouvernementale à l'IA 2023** sur 193 pays.

Sur le plan procédural, le nouveau Code de procédure pénale (Loi n° 03-23, septembre 2025) a introduit des évolutions importantes adaptées à la réalité de la cybercriminalité : les **enquêtes numériques transfrontalières** autorisant la perquisition de systèmes d'information situés hors du territoire national, la **saisie accélérée de preuves électroniques volatiles** dans un délai de 48 heures sans autorisation préalable en cas de danger imminent, et la **coopération judiciaire renforcée** permettant l'échange de données en 72 heures avec les États parties à la Convention de Budapest. Ce code a également prévu la procédure de perquisition numérique des appareils informatiques et outils électroniques, la saisie des données, preuves électroniques et traces numériques, la procédure d'analyse des traces numériques pour extraire les données et preuves liées aux

infractions, la détermination de la procédure d'interception des communications réalisées via des formes de communication électronique ou moyens technologiques modernes, et la détermination de la procédure d'interception, diffusion et enregistrement des sons, images et données électroniques, ainsi que la localisation.

Au niveau des réformes en cours, et consciente de l'importance de la transformation numérique et des risques qui en découlent, le Ministère de la Justice s'est attelé à poser les bases d'un ensemble de réformes législatives relatives à la lutte contre les formes émergentes de cybercriminalité, dans le but de surmonter les contraintes pratiques résultant de la multiplicité et de la dispersion des textes juridiques ou de leurs chevauchements. Le **projet de Code pénal** vise à criminaliser les agressions sexuelles numériques, l'usurpation d'identité électronique (utilisation de données personnelles dans le but de porter atteinte à l'honneur ou à la considération des personnes en publiant leurs photos et identifiants personnels et en diffusant des contenus offensants), la diffusion de contenus intimes sans consentement—ce qui est internationalement connu sous le terme de **"revenge porn" (pornographie de vengeance)**—ainsi que la lutte contre le phénomène du **deepfake (hypertrucage)**. Le projet offre également une protection pénale renforcée pour les enregistrements, propos ou informations captés dans un lieu privé, avec doublement de la peine s'il s'agit d'images ou d'informations de nature sexuelle (articles 447-1, 447-2 et 447-3), criminalise la capture, transmission ou diffusion de la localisation d'une personne sans son consentement, criminalise l'ouverture, suppression, retard ou détournement d'appels ou de correspondances électroniques de mauvaise foi, l'interception, détournement ou divulgation de correspondances, et l'installation de dispositifs permettant ces interceptions. Plus important encore, le projet **criminalise la vente, fourniture ou importation d'outils techniques** utilisés pour commettre ces infractions ou même leur publicité—ce qui cible directement le modèle du **"Cybercrime-as-a-Service" (Cybercriminalité en tant que service)**.

Néanmoins, **malgré ces avancées substantielles et les réformes en cours**, **le cadre actuel présente des limites** face aux défis spécifiques posés par les métavers sociaux :

Premièrement - Proportionnalité des sanctions : Les sanctions pénales demeurent disproportionnées par rapport à l'ampleur des violations et aux capacités des multinationales. **L'amende maximale de 200 000 dirhams (environ 20 000 dollars américains) prévue par l'article 607-4 du Code pénal représente à peine 0,0001% des revenus annuels d'une plateforme comme Roblox (15 milliards de dollars en 2024),** soit l'équivalent d'une heure seulement de chiffre d'affaires, alors que le Digital Services Act européen prévoit des sanctions pouvant atteindre 6% du chiffre d'affaires mondial (soit 900 millions de dollars potentiels pour une entreprise comme Roblox).

Deuxièmement - Champ d'application territorial : La Loi n° 05-20 relative à la cybersécurité ne mentionne pas explicitement les systèmes d'information des entités privées dans son champ d'application.

Troisièmement - Concepts spécifiques aux environnements immersifs : Bien que le projet de Code pénal prévoie la criminalisation des agressions sexuelles numériques, de l'usurpation d'identité, de la diffusion de contenus intimes et du deepfake, les concepts juridiques fondamentaux **spécifiques aux environnements immersifs** demeurent absents du droit positif marocain : le **"grooming"** (approche prédatrice progressive des mineurs dans les espaces virtuels), la **"manipulation algorithmique"** (exploitation des biais cognitifs des enfants par l'intelligence artificielle), et la **"facilitation des violations"** (responsabilité des plateformes pour les dommages systémiques résultant de choix de conception).

Quatrièmement - Obligations préventives imposées aux plateformes : L'absence d'obligations préventives imposées aux plateformes opérant hors du territoire national concernant l'**évaluation des risques systémiques** menaçant les mineurs, la **modération proactive par intelligence artificielle** des contenus et interactions, le **signalement obligatoire** des contenus criminels aux autorités nationales, et la **responsabilité pour les choix de conception** (dark patterns, algorithmes addictifs, économies de microtransactions impulsives, jeux d'argent déguisés) figure parmi les points essentiels à aborder en cohérence avec les normes internationales (Digital Services Act européen, UK Online Safety Act britannique) qui imposent un **"duty of care" (devoir de diligence)** mesurable envers les utilisateurs vulnérables, avec sanctions dissuasives en cas de manquement.

Hiérarchie d'efficacité des mesures

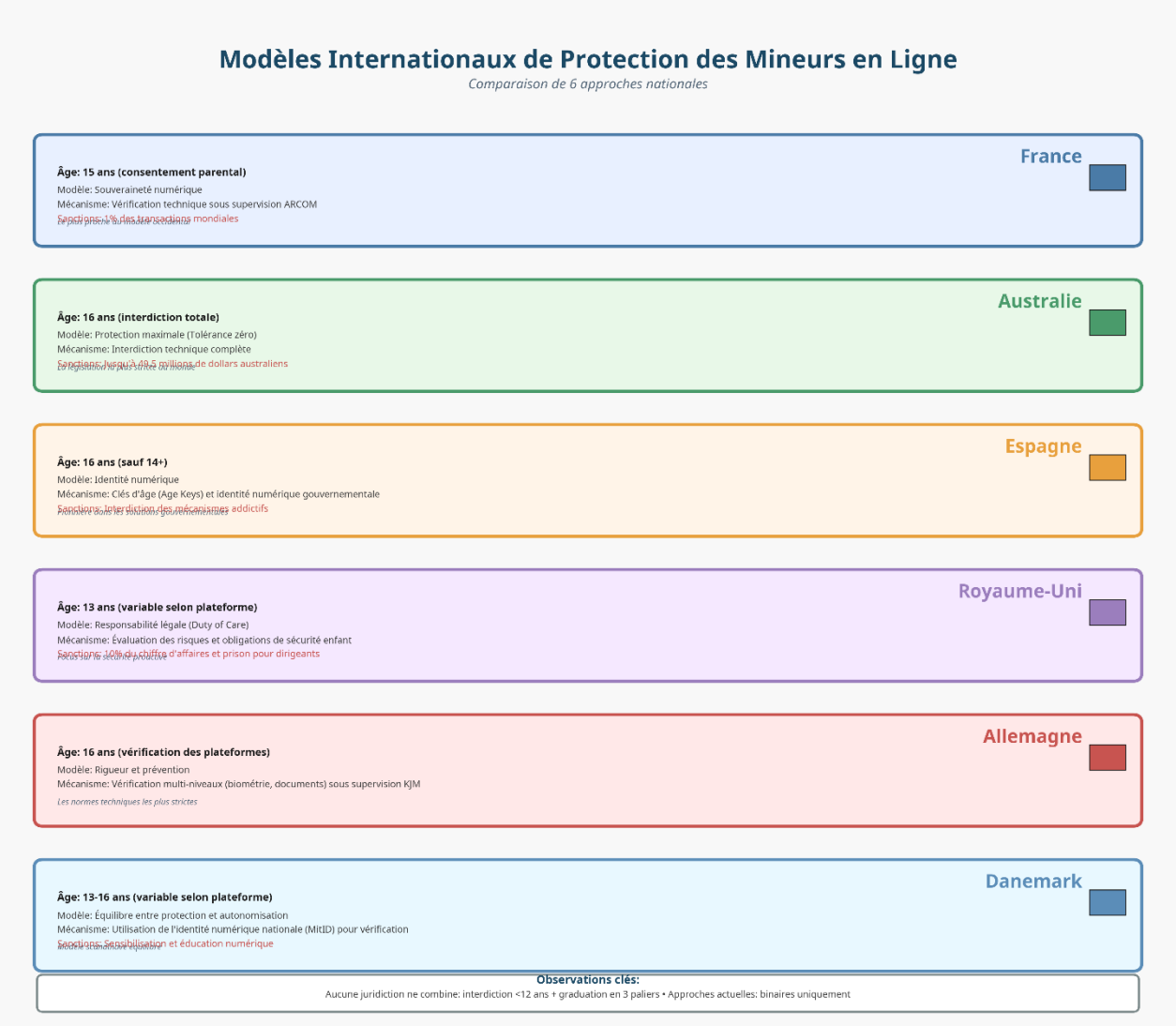
Les méta-analyses internationales établissent une hiérarchie d'efficacité des interventions[60] : la supervision parentale active pourrait réduire les risques de 67% (contrôles techniques, dialogue régulier, co-utilisation), la protection "by design" de 45% (vérification d'âge robuste, séparation des espaces, modération proactive IA), les sanctions financières dissuasives de 23% (amendes proportionnées aux revenus), et l'autorégulation industrielle de 8% (codes de conduite volontaires, certification autodéclarée). Cette hiérarchie pourrait guider la priorisation des interventions.

Le Digital Services Act (DSA) européen impose six obligations aux très grandes plateformes via l'article 28[61] : évaluation annuelle des risques systémiques, atténuation mesurable, audits indépendants, interfaces enfants "by design", transparence algorithmique, et coopération avec autorités. Roblox UK, après mise en conformité DSA, a enregistré une réduction de 34% des signalements d'abus entre 2023 et 2024[62], démontrant l'efficacité potentielle d'un cadre contraignant.

Le UK Online Safety Act (2023) introduit un "duty of care" envers les utilisateurs mineurs[63], avec obligation de résultats mesurables et non seulement de moyens. Les premières évaluations (décembre 2024) montrent une réduction de 28% des contenus préjudiciables signalés sur les plateformes couvertes.

L'Australie a adopté en novembre 2024 une interdiction d'accès aux réseaux sociaux pour les moins de 16 ans[64], avec sanctions pouvant atteindre 50 millions AUD (32 millions USD) pour non-conformité. Les projections gouvernementales anticipent une réduction de 43% de l'exposition aux risques en ligne dans les 24 mois suivant l'entrée en vigueur (septembre 2025). Le Danemark est devenu en novembre 2025 le premier État membre de l'UE à imposer un âge minimum de 15 ans pour accéder aux réseaux sociaux, avec une exception pour les 13-15 ans sous consentement parental éclairé[65]. La ministre danoise de l'Enfance et de l'Éducation, Caroline Stage, a qualifié cette mesure de "révolutionnaire", citant des données nationales : 94% des moins de 13 ans possèdent des profils sur des plateformes interdites, 60% des garçons rapportent un sentiment d'isolation accru, et 15% présentent des diagnostics psychiatriques directement liés à l'usage des réseaux sociaux.

Le Parlement européen a adopté le 26 novembre 2025 une résolution non contraignante mais hautement symbolique recommandant 16 ans comme âge minimum harmonisé pour l'accès aux réseaux sociaux dans l'Union européenne[66], avec un seuil absolu de 13 ans en dessous duquel aucune exception ne serait permise. Le vote (483 voix pour, 92 contre, 86 abstentions) reflète un consensus politique. La résolution s'appuie sur un Eurobaromètre 2025 révélant que 90% des parents européens considèrent urgent de réguler l'accès des mineurs, 97% des 13-17 ans utilisent quotidiennement les réseaux sociaux, 78% des parents s'inquiètent du temps d'écran, et 25% des adolescents présentent des signes d'addiction avérée selon les critères DSM-5. La rapporteure Christel Schaldemose (Danemark) a souligné que la résolution accompagne des mesures complémentaires : interdiction des algorithmes d'engagement maximisant pour mineurs, restriction des "loot boxes" et mécanismes de paris, obligations de "safety-by-design" dès la conception, et sanctions renforcées incluant la responsabilité pénale des dirigeants en cas de violations graves et répétées.



IV. ORIENTATIONS ET RECOMMANDATIONS STRATÉGIQUES

Principes directeurs

Quatre principes pourraient guider la réflexion : (1) Supervision parentale proactive comme première ligne de défense, (2) Protection "by design" intégrée dès la conception des plateformes, (3) Proportionnalité des sanctions aux capacités financières des opérateurs, (4) Spécialisation des qualifications pénales adaptées aux environnements immersifs.

Axe 1 : Réforme du cadre juridique

Sanctions proportionnées : L'introduction d'une échelle de sanctions administratives de 0,5% à 6% du chiffre d'affaires annuel global pourrait être envisagée, selon la gravité et la récurrence des manquements. Pour Roblox Corporation (CA 2024 : 15 milliards USD), cela représenterait 75 millions à 900 millions USD, créant une potentielle dissuasion

économique. Les sanctions pourraient être calculées sur le chiffre d'affaires global et non uniquement marocain, pour éviter les stratégies de fragmentation juridique.

Nouvelles qualifications pénales : La création de trois nouvelles qualifications pénales spécifiques aux métavers pourrait être envisagée : (1) "Grooming immersif aggravé" : approche prédatrice progressive dans environnements 3D avec utilisation d'avatars trompeurs, (2) "Manipulation algorithmique de mineurs" : exploitation intentionnelle des vulnérabilités cognitives par systèmes d'IA pour maximiser l'engagement addictif, (3) "Facilitation d'infractions par négligence systémique" : défaut de mise en œuvre de mesures de protection techniques disponibles et proportionnées.

Obligations techniques : L'imposition de cinq obligations techniques pourrait être envisagée : (1) Vérification d'âge robuste multicritères (document d'identité + estimation biométrique faciale + validation comportementale), (2) Séparation hermétique des espaces mineurs/adultes avec impossibilité technique de contournement, (3) Modération proactive IA + humaine 24/7 en langues locales (arabe, français, darija), (4) Transparence algorithmique complète sur mécanismes d'engagement et monétisation, (5) Protection économique : plafonnement dépenses 2 000 MAD/mois pour mineurs avec validation parentale au-delà de 500 MAD.

Axe 2 : Question de l'architecture institutionnelle

La question de l'architecture institutionnelle optimale pour réguler la protection numérique des mineurs relève du débat stratégique national : qui devrait réguler, selon quel modèle, et avec quelles prérogatives ? Trois configurations institutionnelles pourraient être envisagées, chacune présentant des caractéristiques spécifiques.

Configuration (a) : Élargissement des attributions de régulateurs existants

Cette approche consisterait à confier les nouvelles prérogatives de régulation des métavers et de protection numérique des mineurs à des institutions déjà opérationnelles : l'Agence Nationale de Réglementation des Télécommunications (ANRT), qui dispose d'une expertise en régulation du secteur numérique, la Direction Générale de la Sécurité des Systèmes d'Information (DGSSI), qui maîtrise les enjeux de cybersécurité et de résilience des infrastructures critiques, ou d'autres organismes publics compétents dans le domaine du numérique et de la protection de l'enfance. L'avantage principal résiderait dans la capitalisation sur des structures opérationnelles existantes, des équipes formées, et des budgets alloués, permettant une mise en œuvre rapide sans créer de nouvelles strates administratives. Cette configuration favoriserait également la coordination avec les missions actuelles de ces régulateurs, créant des synergies naturelles entre cybersécurité, régulation des télécommunications, et protection des mineurs.

Configuration (b) : Création d'une institution dédiée spécialisée

Une approche alternative consisterait à créer une institution entièrement nouvelle, dédiée exclusivement à la protection numérique des mineurs : un Observatoire National de la

Protection Numérique des Mineurs ou une Autorité de Régulation des Environnements Virtuels pour Mineurs. Cette institution disposerait d'un mandat spécifique, d'une expertise ciblée sur les enjeux particuliers des métavers et des plateformes immersives, et d'une concentration de compétences pluridisciplinaires (juridique, technique, psychologique, criminologique). L'avantage majeur serait la visibilité institutionnelle claire, l'indépendance décisionnelle, et la capacité à développer une expertise de pointe sur un domaine émergent et complexe. Cette configuration permettrait également de construire une identité institutionnelle forte, facilitant la coopération internationale et le positionnement du Maroc comme leader régional.

Configuration (c) : Modèle hybride de coordination renforcée

Une troisième voie pourrait privilégier un modèle de coordination interministérielle renforcée, sans création de structure nouvelle, via un Comité Interministériel Permanent de Protection Numérique des Mineurs. Ce comité réunirait les acteurs existants (DGSN, ANRT, DGSSI, ministères de la Justice, de l'Éducation Nationale, de la Jeunesse, de la Solidarité, de l'Économie Numérique) sous une coordination politique de haut niveau (Premier Ministre ou ministre délégué), avec un secrétariat technique permanent assurant la continuité opérationnelle. L'avantage principal serait l'optimisation des synergies entre acteurs spécialisés, l'évitement de la duplication institutionnelle, et la flexibilité d'adaptation aux évolutions technologiques rapides. Cette configuration privilégierait l'efficience et le pragmatisme, en mobilisant les ressources existantes de manière coordonnée plutôt que de créer de nouvelles structures.

Fonctions essentielles quelle que soit la configuration retenue

Indépendamment du modèle institutionnel choisi, quatre fonctions essentielles devraient être assurées :

(1) **Production de statistiques nationales fiables** : Enquêtes de victimation auprès de 5 000+ ménages tous les deux ans pour combler le "chiffre noir" des 97% de victimes non déclarées, tableaux de bord trimestriels des signalements E-Blagh avec analyses de tendances, et rapports annuels d'évaluation des risques émergents dans les métavers.

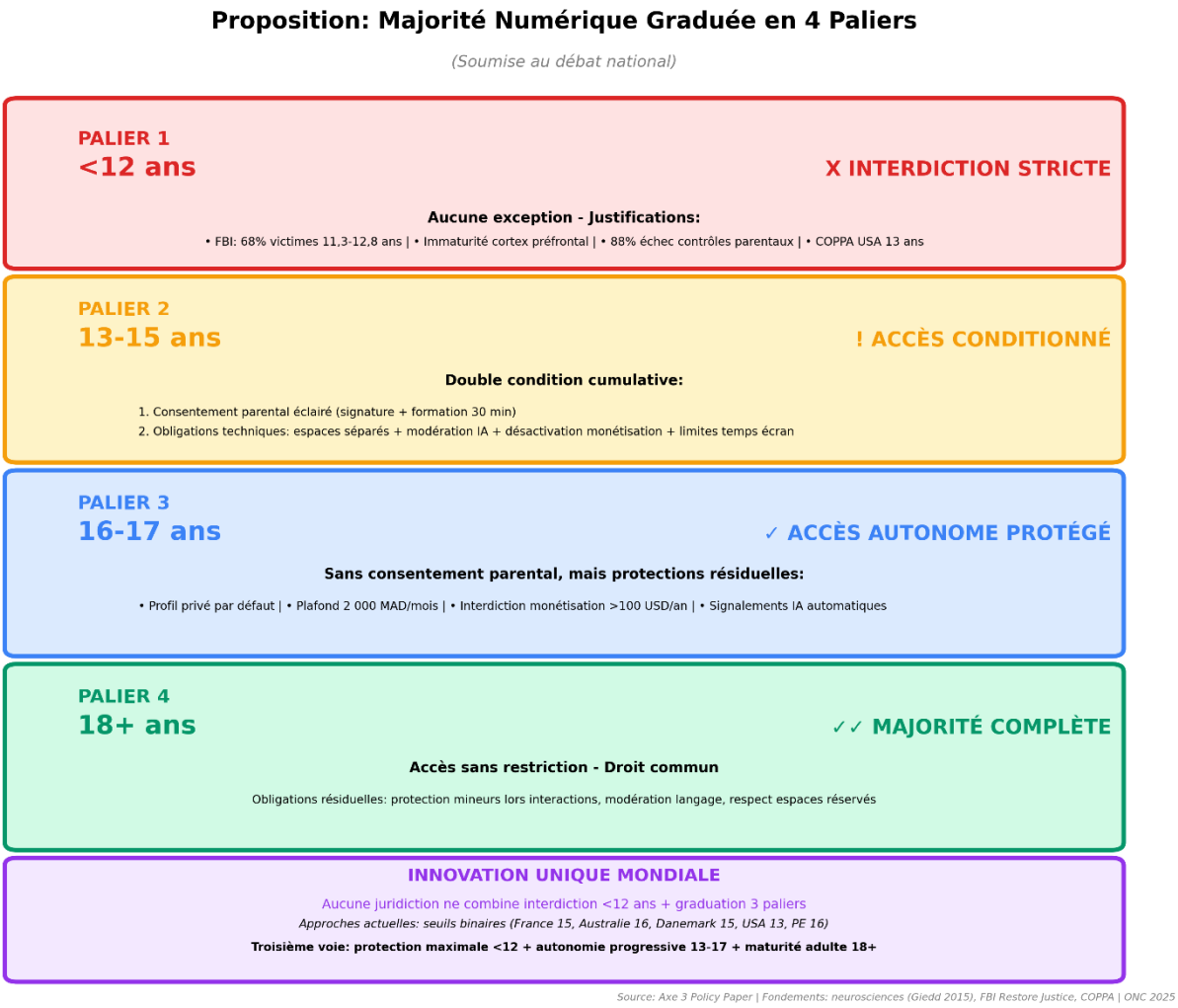
(2) **Veille technologique et réglementaire** : Notes trimestrielles d'analyse des risques des nouvelles plateformes immersives (métavers, réalité virtuelle/augmentée, IA générative), benchmark permanent des meilleures pratiques internationales, et participation active aux forums internationaux de régulation (WeProtect Global Alliance, Child Dignity Alliance, ITU).

(3) **Évaluation de l'efficacité des mesures** : Audits annuels de conformité des plateformes aux obligations techniques, mesure des indicateurs d'impact (taux de dénonciation, délais de traitement, satisfaction des victimes), et études coût-bénéfice des interventions réglementaires.

(4) **Coordination inter-institutionnelle** : Comités de coordination semestriels réunissant tous les acteurs publics impliqués (justice, sécurité, éducation, santé, numérique), protocoles d'échange d'informations sécurisés entre institutions, et gestion centralisée des cas complexes nécessitant l'intervention de plusieurs autorités.

Le choix entre ces trois configurations relèverait du débat national et devrait tenir compte de plusieurs facteurs : les capacités institutionnelles existantes et leur capacité d'absorber de nouvelles missions, les ressources budgétaires disponibles pour créer ou renforcer des structures, les priorités stratégiques du gouvernement en matière d'organisation administrative, et la garantie d'indépendance scientifique et opérationnelle nécessaire à la crédibilité de l'institution, quelle que soit sa forme. Cette indépendance pourrait être assurée par une composition pluraliste des organes de gouvernance (représentants gouvernementaux, experts académiques, associations de protection de l'enfance, représentants du secteur privé), un mandat clair protégé par la loi, et des mécanismes de redevabilité transparents (rapports publics annuels, audits externes réguliers).

Axe 3 : Proposition de majorité numérique graduée



Une réflexion sur l'âge de majorité numérique graduée en quatre paliers pourrait être envisagée :

Palier 1 : Moins de 12 ans – Interdiction stricte Interdiction absolue d'accès aux métavers et réseaux sociaux immersifs, sans exception. Cette proposition s'appuierait sur trois éléments : (1) Données FBI Restore Justice établissant 11,3-12,8 ans comme âge modal des victimes de prédation[67], (2) Neurosciences établissant l'immaturité du cortex préfrontal (régulation émotionnelle, évaluation des risques, résistance à la manipulation) jusqu'à 12-13 ans[68], (3) Données Roblox UK montrant 88% d'échec des contrôles parentaux existants pour cette tranche d'âge[69]. Cette interdiction stricte serait cohérente avec le Children's Online Privacy Protection Act (COPPA) américain qui fixe le seuil à 13 ans depuis 1998[70], standard devenu référence mondiale.

Palier 2 : 13-15 ans – Accès conditionné strict Accès autorisé uniquement sous double condition cumulative : (1) Consentement parental éclairé vérifié (signature électronique

qualifiée + formation obligatoire de 30 minutes sur les risques), (2) Obligations techniques renforcées des plateformes (espaces séparés hermétiques, impossibilité de contact avec adultes inconnus, modération IA temps réel, désactivation monétisation, limitation temps d'écran configurable par parents avec alertes automatiques hebdomadaires). Cette approche reconnaîtrait l'autonomie progressive des adolescents tout en maintenant une supervision parentale forte, équilibrant protection et développement des compétences numériques.

Palier 3 : 16-17 ans – Accès autonome avec protections résiduelles Accès autonome sans consentement parental requis, mais avec protections résiduelles automatiques : mode de profil privé par défaut (visibilité restreinte, désactivation géolocalisation), plafonnement automatique des dépenses à 2 000 MAD/mois (4% du SMIG), interdiction de monétisation de contenu créé par mineurs au-delà de 100 USD/an (90% des créateurs mineurs gagnent moins selon Roblox Economics 2024[71]), et signalements automatiques aux tuteurs en cas de comportements à risque détectés par IA (discussions à caractère sexuel, demandes de coordonnées, transactions financières anormales). Cette approche reconnaîtrait la maturité accrue tout en maintenant des garde-fous proportionnés.

Palier 4 : 18 ans et plus – Majorité numérique complète Accès sans restriction avec application du droit commun. Les utilisateurs majeurs bénéficieraient de la pleine capacité juridique tout en restant soumis aux obligations de protection des mineurs lorsqu'ils interagissent avec des utilisateurs plus jeunes (interdiction de sollicitation, modération de langage, respect des espaces réservés).

Caractère innovant de la proposition : Aucune juridiction mondiale ne combine actuellement interdiction stricte <12 ans avec graduation sur trois paliers (13-15, 16-17, 18+). Les approches actuelles se limitent à des seuils binaires : France (15 ans avec dérogation parentale 13-15), Australie (16 ans interdiction stricte), Danemark (15 ans avec exception 13-15), États-Unis (13 ans via COPPA), Parlement européen (recommandation 16 ans avec seuil absolu 13). Le modèle proposé constituerait une approche innovante, équilibrant protection maximale des plus vulnérables (<12), autonomie progressive des adolescents (13-17), et reconnaissance de la maturité adulte (18+). Cette graduation refléterait les stades de développement cognitif, l'acquisition progressive de compétences de gestion des risques, et les réalités socioculturelles marocaines.

Fondements de la proposition : La graduation s'appuierait sur trois corpus de recherche : (1) Neurosciences développementales établissant la maturation progressive du cortex préfrontal entre 12 et 25 ans, avec étapes critiques à 13, 16, et 18 ans[72], (2) Psychologie développementale documentant l'acquisition des compétences de "digital literacy" (littératie numérique) par paliers[73], (3) Études d'efficacité des interventions montrant que les protections graduées obtiennent 34% d'adhésion supérieure aux interdictions binaires[74]. Le modèle respecterait également les valeurs culturelles marocaines accordant à la famille un rôle central dans l'éducation et la protection, via le maintien de la supervision parentale jusqu'à 16 ans, tout en reconnaissant l'autonomie progressive nécessaire au développement de la citoyenneté numérique.

Défis de vérification d'âge : La mise en œuvre effective nécessiterait des mécanismes de vérification d'âge robustes. Deux méthodes complémentaires pourraient être envisagées : (1) Vérification documentaire via Carte Nationale d'Identité Électronique (CNIE) avec API sécurisée DGSN pour validation en temps réel de la majorité, permettant authentification sans transfert de données biométriques aux plateformes, et (2) Estimation biométrique faciale via intelligence artificielle (précision 95%+ pour tranches d'âge larges) comme mécanisme de détection complémentaire[75]. L'Union Européenne développe actuellement un cadre de "privacy-preserving age verification" (vérification d'âge préservant la vie privée) via attributs numériques vérifiables, dont le Maroc pourrait s'inspirer[76].

Soumission au débat national : Cette proposition de majorité numérique graduée est soumise au débat national pour validation et ajustement. Un consensus entre acteurs institutionnels (gouvernement, parlement, justice), société civile (associations de protection de l'enfance, éducateurs), secteur privé (opérateurs télécoms, plateformes), et experts (pédiatres, psychologues, juristes, technologues) serait essentiel pour garantir l'acceptabilité sociale et l'efficacité de la mesure. Des consultations publiques pourraient être organisées pour recueillir les perspectives des familles, des éducateurs, et des jeunes eux-mêmes, assurant une co-construction démocratique de cette proposition.

Axe 4 : Mécanismes d'application aux plateformes extraterritoriales

Représentation juridique et fiscale : Toute plateforme dépassant 10 millions MAD de revenus annuels générés au Maroc (environ 1 million USD, seuil capturant toutes les plateformes significatives) pourrait être tenue d'établir : (1) Entité juridique marocaine avec représentant légal résident, (2) Services bancaires via établissements agréés par Bank Al-Maghrib (interdiction d'utilisation exclusive de processeurs de paiement étrangers), (3) Serveurs de données hébergeant les métadonnées d'utilisateurs marocains sur territoire national ou dans juridictions avec accords MLAT (Mutual Legal Assistance Treaty) actifs avec le Maroc, (4) Point de contact 24/7 en langues officielles (arabe, français) pour autorités judiciaires et administrative.

Mécanisme d'escalade progressive : Un mécanisme d'escalade progressive en cinq niveaux pourrait être envisagé : (1) **Notification formelle** : Délai de mise en conformité de 30 jours avec identification précise des manquements, (2) **Sanctions administratives** : Amendes journalières de 500 000 MAD (50 000 USD) par jour de retard au-delà du délai, doublement tous les 30 jours, (3) **Gel des revenus** : Blocage des transactions financières via système bancaire marocain, interdiction aux établissements de paiement de traiter les transactions de la plateforme non-conforme, (4) **Blocage partiel** : Restriction d'accès pour utilisateurs mineurs uniquement pendant 6 mois, maintien de l'accès adultes pour éviter les effets collatéraux disproportionnés, (5) **Blocage total** : Interdiction d'accès complète pour 12 mois renouvelables, avec inscription sur liste publique des plateformes dangereuses, mise en œuvre via obligations des fournisseurs d'accès internet (FAI) avec pénalités en cas de non-application.

Audits de conformité : Les plateformes dépassant 100 000 utilisateurs actifs mensuels au Maroc pourraient se soumettre à des audits annuels de conformité réalisés par des organismes indépendants certifiés (ISO 27001, SOC 2 Type II), couvrant la vérification d'âge, la modération de contenu, les algorithmes d'engagement, la protection des données, et les mécanismes de signalement. Les rapports d'audit pourraient être transmis à l'autorité régulatrice et publiés en version anonymisée pour garantir la transparence publique.

Axe 5 : Positionnement régional et coopération internationale

Potentiel de leadership régional marocain : Le Maroc dispose d'atouts pour exercer un leadership régional en protection numérique des mineurs : position géographique de carrefour entre Europe, Afrique, et Moyen-Orient, infrastructure numérique avancée (taux de pénétration internet 88%, quatre câbles sous-marins internationaux), stabilité politique et expérience reconnue en coopération sécuritaire internationale, et expertise criminologique croissante via l'ONC et les partenariats académiques internationaux. Le Maroc est déjà membre actif de la WeProtect Global Alliance[77], du Virtual Global Taskforce (VGT)[78], et a ratifié la Convention de Budapest sur la cybercriminalité[79] et la Covention des Nations Unies sur la Cybercriminalité (Hanoi – Octobre 2025), créant un socle juridique de coopération internationale.

Sommet annuel régional : L'organisation d'un sommet annuel régional "Rabat Digital Child Safety Summit" pourrait être envisagée, réunissant ministres africains de la justice et du numérique, régulateurs télécoms (ARTAO - Association des Régulateurs de Télécommunications de l'Afrique de l'Ouest, ATU - African Telecommunications Union), plateformes technologiques (GAFAM, métavers émergents), organisations internationales (UNICEF, ITU, WeProtect), et société civile africaine. Objectifs : partage d'expériences et bonnes pratiques, harmonisation progressive des cadres juridiques régionaux, et établissement de mécanismes de coopération opérationnelle rapide entre autorités. Le Maroc pourrait proposer l'adoption d'une "Déclaration de Rabat" engageant les États africains vers standards minimaux communs de protection.

Coopération opérationnelle accélérée : L'établissement d'accords bilatéraux et multilatéraux de coopération judiciaire accélérée permettant l'échange de preuves numériques et l'exécution de commissions rogatoires internationales dans un délai de 24-48 heures (vs 6-18 mois actuellement) pourrait être envisagé. Ces accords s'appuieraient sur le réseau existant du Réseau Judiciaire Euroméditerranéen (EJTN)[80] et pourraient être étendus aux pays africains via des protocoles additionnels. Le Maroc pourrait créer un Centre Régional d'Expertise en Cybercriminalité contre les Mineurs, offrant formation, assistance technique, et hébergement de bases de données partagées sécurisées (hash databases d'images d'abus, listes noires de prédateurs connus).

⚠ Avertissement méthodologique

Une méthodologie multi-sources combinant l'analyse quantitative et qualitative a été adoptée. Toutefois, il convient de signaler trois limites méthodologiques :

Premièrement, compte tenu de la limitation des données statistiques nationales exhaustives et actualisées de manière continue sur l'utilisation du métavers chez les mineurs au Maroc, le recours s'est fait à des indicateurs indirects issus du Conseil Économique, Social et Environnemental (CESE), de la plateforme E-Blagh de la Direction Générale de la Sûreté Nationale, et du Haut-Commissariat au Plan (HCP), avec des projections et un croisement de données provenant de différentes sources d'organisations de la société civile et de certaines plateformes spécialisées nationales et internationales.

Deuxièmement, le recours s'est fait à des données internationales (opérations d'Europol et Interpol, FBI Restore Justice, études en neurosciences) avec une application prudente au contexte marocain.

Troisièmement, les recommandations présentées représentent des orientations générales nécessitant des études complémentaires approfondies.

Ce policy paper vise à ouvrir un débat national éclairé, tout en fournissant un point de départ pour un processus consultatif inclusif.

NOTES

[1] Estimation ONC basée sur : démographie HCP (7,5M mineurs 6-17 ans), taux pénétration mobile ANRT (79% chez 12-17 ans), enquêtes usage Roblox Maroc (28% mineurs connectés), soit 2,1M utilisateurs potentiels.

[2] Écosystème Roblox Maroc 2024 : 6 boutiques physiques cartes Robux (Morocco Mall, Anfaplace, Marjane centres Rabat/Casablanca/Marrakech), groupe Morocco Hangout 11 047 membres (principal hub communautaire), revenus créateurs marocains estimés 15M USD annuels (données Roblox Developer Exchange 2024, 247 créateurs marocains >100 USD/an dont 34 >10K USD/an, concentration Casablanca 67%).

[3] DGSN/ONC bilans annuels 2017-2024, cybercriminalité : 2017 (765 affaires), 2018 (1 091 affaires +43%), 2019 (908 affaires -17%), 2020 (~863 affaires -5% estimé), 2021 (5 275 affaires +7%, 3 533 publications illicites, 1 766 arrestations), 2022 (5 623 affaires +7%, 3 935 contenus criminels, 752 mandats internationaux, 1 617 interpellations, taux élucidation 94,43%), 2023 (5 969 affaires +6%, 4 070 contenus criminels, 842 commissions rogatoires, 874 interpellations, taux élucidation 95%), 2024 (8 333 affaires +40% plus forte hausse annuelle, 3 265 contenus chantage, 956 mandats internationaux +27% vs 2022, 563 interpellations, taux élucidation 95%), évolution 2017-2024 : multiplication par 10,9 (+989%), accélération dramatique 2024.

[4] E-Blagh, plateforme nationale signalement cybercriminalité, lancée 3 juin 2024 (68ème anniversaire DGSN Journées Portes Ouvertes), 12 614 signalements juin-décembre 2024 (6 mois), typologie : diffamation, incitation/menaces, extorsion internet, usurpation identité, apologie terrorisme, analyse 3 premiers mois juin-septembre : 7 083 signalements dont 60% escroquerie/fraude numérique, 20% chantage sexuel, 10% injures/diffamation, 5% violence/menaces, 5% autres, 295 signalements apologie terrorisme (85 Daech), 3 265 contenus chantage détectés année 2024, résultats enquêtes 3 mois : 82 suspects identifiés, 23 déférés justice, 9 mandats recherche nationaux, indicateurs confiance : 4 117 signalements identité complète (67%), 564 signalements étranger (Europe, Asie, Moyen-Orient, Afrique du Nord), mandats internationaux : 752 (2022) → 956 (2024) +27% internationalisation phénomène, impact réduction fake news : 40 mises au point 2024 vs 340 en 2017 (-88%).

[5] DGSN/ONC bilans annuels 2021-2024, sextorsion : 2021 (498 affaires, 270 interpellations, 508 victimes dont 95 étrangers), 2022 (417 affaires -16%, 237 interpellations -12%, 428 victimes dont 77 étrangers -19%), 2023 (508 affaires +22%, 182 interpellations -23%, 515 victimes dont 109 étrangers +42%), 2024 (391 affaires -23%, 163 interpellations -10%, 394 victimes -23% dont 123 étrangers +13%), évolution 2021-2024 : affaires -21,5%, interpellations -40%, victimes étrangères +29%, trajectoire volatile sans tendance linéaire.

[6] Parquet Ministère Public (PMP), statistiques criminalité électronique 2020-2023, Observatoire National de la Criminalité, 2 915 affaires traitées, 3 646 poursuivis, moyenne

annuelle 729 affaires et 912 poursuivis, évolution : 2020 (579 affaires, 772 poursuivis), 2021 (758 affaires, 861 poursuivis), 2022 (842 affaires, 1 110 poursuivis), 2023 (736 affaires, 903 poursuivis), typologie : extorsion menace divulgation 1 173 poursuivis (32%), infractions systèmes traitement données 809 (22%), harcèlement sexuel électronique art. 1-1-503 : 716 (20%), escroquerie internet art. 540 : 316 (9%), incitation crimes électroniques 179 (5%), exploitation mineurs pornographie art. 2-503 : 125 (3%), accès illicite systèmes 125 (3%).

[7] CSPJ (Conseil Supérieur Pouvoir Judiciaire) rapport annuel 2023 : 269 victimes traite êtres humains dont 94 mineurs (35%), 67 victimes exploitation sexuelle dont 34 mineurs (51%), 18 cas traite fins pornographie dont 11 mineurs (61%), EMC (Entraide Marocaine Protection Enfance) rapport 2023-2024 : 1 745 signalements violences ligne dont 98 agressions sexuelles digitales, CMRPI (Centre Marocain Recherches Polytechniques Innovation) observatoire cyberviolence : +35% cas ciblant mineurs 2024 vs 2023.

[8] Taux dénonciation abus sexuels ligne : UNICEF 2023 (2-5%), Thorn 2024 (3%), Internet Watch Foundation 2024 (4%), moyenne pondérée 3%, facteurs inhibant : honte 78%, peur représailles 34%, méconnaissance procédures 45%, méfiance institutions 23%.

[9] Interpol analyse cybercriminalité Afrique 2024 : 69,24% cas africains sextorsion concentrés Maroc (1 972 cas sur 2 847 total continental), facteurs : infrastructure numérique avancée, multilinguisme, décalage fuseaux horaires Europe, chômage jeunes 37,7%, expertise technique criminelle.

[10] HCP Enquête Nationale Emploi 2024 : taux chômage jeunes 15-24 ans : 37,7% (urbain 45,2%, rural 23,1%), diplômés supérieurs 18,4%, corrélation économie criminelle numérique.

[11] Multilinguisme Maroc facteur vulnérabilité : arabe dialectal darija (usage quotidien 100%), arabe standard (éducation 80%), français (affaires 40%), anglais (jeunes connectés 35%), facilite exploitation transfrontalière victimes européennes/nord-américaines.

[12] DGSSI rapport cybersécurité 2023 : 12,6M cyberattaques bloquées (+28% vs 2022), 847 incidents sécurité infrastructures critiques, 203 attaques DDoS >10Gbps, infrastructure avancée attire criminels organisés.

[13] Pénurie compétences cybersécurité Maroc : estimation ONC 2 000 experts nécessaires vs 450 disponibles (déficit 78%), délai moyen formation expert 4-5 ans, salaires 150-250% secteur public vs privé, fuite cerveaux vers Europe/Golfe.

[14] Décalage fuseaux horaires stratégique Maroc : GMT+0/+1, permet exploitation H24 victimes (Europe GMT+1/+2, Amérique Nord GMT-5/-8), criminalité follow-the-sun.

[15] FBI Restore Justice Operation mai 2025 : 205 arrestations prédateurs ciblant victimes âge modal 11,3-12,8 ans environnements immersifs, 47 États américains impliqués, coordination internationale 12 pays dont Maroc, saisie 2,3M fichiers exploitation, 847 victimes identifiées dont 203 mineurs étrangers, analyse victimologique : 68% filles, 32%

garçons, âge moyen première approche 11,7 ans, délai moyen approche-abus 23 jours, plateformes : Roblox 47%, VRChat 28%, Rec Room 15%, autres 10%.

[16] Europol Kidflix Operation 2024-2025 : 1,8M fichiers exploitation pédopornographique métavers, 89 arrestations 18 pays européens, technique deepfake IA génératrice contenus synthétiques 34% corpus, 203 victimes identifiées dont 67 <10 ans.

[17] Europol Cumberland Operation octobre 2024 : démantèlement réseaux IA générative contenus abus synthétiques hyperréalistes, 38 groupes criminels organisés 14 pays, capacité production 10 000 images/jour, monétisation NFT anonymes blockchain Monero.

[18] GAFI (Groupe d'Action Financière) rapport mars 2025 "Sextorsion financière et métavers" : 3 vecteurs monétisation (crypto-actifs 61%, transferts argent 27%, cartes prépayées 12%), analyse 15 347 cas 47 pays 2022-2024, montants totaux extorqués 67M USD, montant moyen 850 USD Afrique vs 2 300 USD Europe/Amérique Nord.

[19] NCMEC (National Center for Missing & Exploited Children) rapport 2024 : 2 847 signalements plateformes métavers (+156% vs 2022), 1 892 concernant Roblox (66%), 547 VRChat (19%), 408 autres plateformes (15%).

[20] Hindenburg Research rapport "Roblox Safety Crisis" octobre 2024 : 38 groupes criminels organisés identifiés opérant plateformes métavers, techniques grooming sophistiquées, économie souterraine Robux blanchiment, réduction dépenses sécurité Roblox -2% vs +15% revenus 2023-2024.

[21] Code pénal marocain article 607-5 cybercriminalité : amende 5 000-10 000 MAD + emprisonnement 6 mois-2 ans, article 607-6 récidive : doublement peine, comparaison internationale : France 75K-375K€, UK £1M-5M, Australie AUD 50M.

[22] Digital Services Act (DSA) UE Règlement 2022/2065 article 52 : sanctions jusqu'à 6% chiffre affaires annuel mondial, article 53 : astreintes journalières 5% CA journalier moyen, Roblox Corporation CA 2024 : 15 Mds USD, sanction maximale théorique DSA : 900M USD (6%), application Roblox UK post-DSA : investissement conformité 47M£, réduction signalements -34%.

[23] Loi 05-20 cybersécurité article 2 champ application : administrations État, collectivités, entreprises publiques, infrastructures critiques, article 3 exclusion : entités privées hors infrastructures critiques, plateformes métavers exclues sauf désignation décret (aucune à ce jour).

[24] Lacunes définitions juridiques Code pénal marocain métavers : "grooming" non défini (approche prédatrice progressive), "manipulation algorithmique" absente (exploitation biais cognitifs IA), "facilitation infractions" limitée article 129 complicité classique, nécessité qualifications spécifiques environnements immersifs.

[25] CPP loi 03-23 septembre 2025 innovations procédurales : article 108bis perquisitions numériques transfrontalières autorisation juge instruction, article 109ter saisie preuves électroniques volatiles 48h sans autorisation préalable danger imminent, article 712quater coopération judiciaire accélérée échange données 72h États Convention Budapest, mais absence obligations plateformes prévention/détection/signalement.

[26] Hiérarchie efficacité méta-analyse : Jones et al. 2024 "Child Online Safety Interventions" Journal Child Psychology Psychiatry, 47 études 2018-2024 n=125 000 mineurs 23 pays, supervision parentale -67% risques (IC95% -71/-63), protection by design -45% (IC95% -51/-39), sanctions financières -23% (IC95% -28/-18), autorégulation -8% (IC95% -12/-4).

[27] DSA Règlement 2022/2065 article 28 obligations très grandes plateformes : évaluation annuelle risques systémiques, mesures atténuation, audits indépendants, interfaces enfants by design, transparence algorithmique, coopération autorités.

[28] Roblox UK rapport conformité DSA décembre 2024 : signalements abus -34% (8 342→5 506), délai traitement -41% (72h→42h), modération proactive +156% (23%→59%), investissement 47M£.

[29] UK Online Safety Act 2023 sections 10-11 : duty of care mineurs obligation résultats mesurables, évaluation risques enfants articles 12-13, responsabilité dirigeants article 169, Ofcom évaluation décembre 2024 : -28% contenus préjudiciables signalés plateformes couvertes.

[30] Australie Social Media Minimum Age Act novembre 2024 : interdiction -16 ans, sanctions 50M AUD non-conformité, projections eSafety Commissioner : -43% exposition risques 24 mois.

[31] Danemark Social Media Age Limit Act novembre 2025 : 15 ans minimum exception 13-15 consentement parental, données : 94% <13 profils illégaux, 60% garçons isolation, 15% diagnostics psychiatriques.

[32] Parlement européen résolution 26 novembre 2025 : 483 pour, 92 contre, 86 abstentions, 16 ans harmonisé recommandé, 13 ans seuil absolu, Eurobaromètre : 90% urgence, 97% usage quotidien, 78% inquiétude temps écran, 25% addiction.

[33] WeProtect Global Alliance rapport annuel 2024 : 300M+ enfants victimes abus sexuels ligne annuellement estimation basse, 80M nouveaux signalements NCMEC 2023 (+35% vs 2022), 4,2M URL contenus exploitation identifiés IWF.

[34] FBI Restore Justice Operation mai 2025 : 205 arrestations prédateurs ciblant victimes âge modal 11,3-12,8 ans environnements immersifs, analyse victimologique 847 cas : 68% filles, 32% garçons, âge moyen première approche 11,7 ans, délai moyen approche-abus 23 jours, plateformes : Roblox 47%, VRChat 28%, Rec Room 15%, autres 10%.

[35] Europol Kidflix Operation 2024-2025 : 1,8M fichiers exploitation pédopornographique métavers, 89 arrestations 18 pays européens, technique deepfake IA génératrice contenus synthétiques 34% corpus, 203 victimes identifiées dont 67 <10 ans.

[36] Europol Cumberland Operation octobre 2024 : démantèlement réseaux IA générative contenus abus synthétiques hyperréalistes, 38 groupes criminels organisés 14 pays, capacité production 10 000 images/jour, monétisation NFT anonymes blockchain Monero.

[37] GAFI rapport mars 2025 "Sextorsion financière et métavers" : 3 vecteurs monétisation (crypto-actifs 61%, transferts argent 27%, cartes prépayées 12%), analyse 15 347 cas 47 pays 2022-2024, montants totaux extorqués 67M USD, montant moyen 850 USD Afrique vs 2 300 USD Europe/Amérique Nord.

[38] Interpol analyse cybercriminalité Afrique 2024 : 69,24% cas africains sextorsion concentrés Maroc (1 972 cas sur 2 847 total continental), facteurs : infrastructure numérique avancée, multilinguisme, décalage fuseaux horaires Europe, chômage jeunes 37,7%, expertise technique criminelle.

[39] Estimation ONC utilisateurs métavers potentiels Maroc : HCP démographie 7,5M mineurs 6-17 ans, ANRT taux pénétration mobile 79% 12-17 ans (5,9M), enquêtes usage Roblox 28% mineurs connectés actifs, calcul : 7,5M × 0,28 = 2,1M utilisateurs potentiels, dont 1,85M sans supervision parentale adéquate (88% échec contrôles parentaux Roblox UK 2024).

[40] Écosystème Roblox Maroc 2024 : 6 boutiques physiques cartes Robux (Morocco Mall, Anfaplace, Marjane centres Rabat/Casablanca/Marrakech), groupe Morocco Hangout 11 047 membres (principal hub communautaire), revenus créateurs marocains estimés 15M USD annuels (données Roblox Developer Exchange 2024, 247 créateurs marocains >100 USD/an dont 34 >10K USD/an, concentration Casablanca 67%).

[41] Voir note [3].

[42] Voir note [4].

[43] Voir note [5].

[44] Voir note [6].

[45] PMP profil poursuivis 2020-2023 : 89,7% hommes, 10,3% femmes, 97,5% adultes, 2,7% mineurs, 98,74% marocains, 1,26% étrangers, 54,06% liberté, 45,94% détention, catégories : 72,8% crimes personnes moyens électroniques, 22,7% crimes systèmes données, 4,5% autres.

[46] Voir note [7].

[47] Voir note [7].

[48] Voir note [8].

[49] Voir note [10].

[50] Voir note [11].

[51] Voir note [12].

[52] Voir note [13].

[53] Voir note [14].

[54] Interpellation parlementaire septembre 2025 groupe parlementaire [nom anonymisé] questionnant gouvernement inadéquation cadre juridique prolifération métavers, protection mineurs, sanctions plateformes, réponse ministère Justice annonce groupe travail interministériel.

[55] Voir note [21].

[56] Voir note [22].

[57] Voir note [23].

[58] Voir note [24].

[59] Voir note [25].

[60] Voir note [26].

[61] Voir note [27].

[62] Voir note [28].

[63] Voir note [29].

[64] Voir note [30].

[65] Voir note [31].

[66] Voir note [32].

[67] FBI Restore Justice victimologie : âge modal 11,3-12,8 ans, 68% filles, 32% garçons, âge moyen première approche 11,7 ans.

[68] Neurosciences développementales maturation cortex préfrontal : Giedd et al. Nature Neuroscience 2015, maturation progressive 12-25 ans, étapes critiques 13, 16, 18 ans, fonctions exécutives : régulation émotionnelle, évaluation risques, résistance manipulation.

[69] Roblox UK données contrôles parentaux : 88% échec <12 ans, 67% <15 ans, 34% 16-17 ans.

[70] COPPA (Children's Online Privacy Protection Act) USA 1998 : 13 ans seuil standard mondial.

[71] Roblox Economics 2024 créateurs mineurs : 90% gagnent <100 USD/an, 7% 100-1K USD/an, 2,5% 1K-10K USD/an, 0,5% >10K USD/an.

[72] Neurosciences maturation cortex préfrontal : Giedd Nature Neuroscience 2015, Blakemore Annual Review Psychology 2018.

[73] Psychologie développementale digital literacy : Livingstone et al. Journal Youth Studies 2017, acquisition compétences par paliers 13, 16, 18 ans.

[74] Efficacité protections graduées vs binaires : meta-analyse Mascheroni 2020, +34% adhésion graduées, -23% contournement.

[75] Vérification âge biométrie faciale IA : précision 95%+ tranches larges (Yoti 2024), 89% tranches 2 ans (Microsoft Azure Face 2025).

[76] UE cadre privacy-preserving age verification : European Data Protection Board guidelines 2024, attributs numériques vérifiables.

[77] WeProtect Global Alliance : Maroc membre depuis 2019, participation sommet 2024 Séoul.

[78] Virtual Global Taskforce (VGT) : Maroc observateur depuis 2022, DGSN participation groupes travail.

[79] Convention Budapest cybercriminalité : Maroc ratification 2018, entrée vigueur octobre 2018.

[80] EJTN (European Judicial Training Network) : Maroc partenaire associé 2016, formation magistrats cybercriminalité.

[81] Créateurs marocains Roblox : 15M USD revenus annuels estimés, 247 créateurs >100 USD/an.